

**IN THE CLAIMS:**

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 1, 2, and 15-48, AMEND claims 3, 12-14, 49, and 50 in accordance with the following:

1-2. (CANCELLED)

3. (CURRENTLY AMENDED) A security method of a network accessible apparatus, the security method comprising:

generating a context based on application content received by the network accessible apparatus;

identifying whether the context is a reliable context or an unreliable context, wherein the context issues a command to perform a specific operation;

determining that the specific operation is not permitted when the context is an unreliable context; and

not performing the specific operation and outputting an error message when the specific operation is not permitted;

wherein the identifying of whether the context is a reliable context of an unreliable context comprises identifying the context as a reliable context is the command includes an "http://" request, and identifying the context as an unreliable context if the command includes an "https://" request.

4. (ORIGINAL) The security method of claim 3, wherein the issuing of the command comprises identifying a reliability of the context based on a flag of a memory into which the context that issues the command is loaded.

5. (ORIGINAL) The security method of claim 3, further comprising:

not performing a preload when the context commands to preload a markup document to secure seamless reproduction of AV data and outputting the error message.

6. (ORIGINAL) The security method of claim 3, further comprising:  
not performing a deletion when the context commands to delete data that is preloaded in a memory of the network accessible apparatus and outputting the error message.

7. (ORIGINAL) The security method of claim 3, further comprising:  
not performing access when the context commands to access data that is recorded on a disk mounted in the network accessible apparatus and outputting the error message.

8. (ORIGINAL) The security method of claim 3, further comprising:  
not performing access when the context commands to access another frame through a frame and outputting the error message.

9. (ORIGINAL) The security method of claim 3, further comprising:  
not performing access when the context commands to access cookies that are stored in the network accessible apparatus by another context and outputting the error message.

10. (ORIGINAL) The security method of claim 3, further comprising:  
not performing access when the context commands to access another context that is operated in the network accessible apparatus and outputting the error message.

11. (ORIGINAL) The security method of claim 3, further comprising:  
not performing control when the context commands to control a reproducing engine, which reproduces AV data recorded on a disk mounted in the network accessible apparatus and outputting the error message.

12. (CURRENTLY AMENDED) A security method of a network accessible apparatus, the security method comprising:  
issuing a command by a first reliable context to read application content;  
identifying whether the command is a reliable request or an unreliable request based on syntax of the command; and

generating a second reliable context corresponding to the application content and accessing the application content according to the second reliable context when the command is the reliable request; and

generating an unreliable context and accessing the application content according to the unreliable context when the command is the unreliable request.

13. (CURRENTLY AMENDED) The security method of claim 12, wherein the application content corresponding to the second reliable context is recorded on a disk mounted in the network accessible apparatus.

14. (CURRENTLY AMENDED) The security method of claim 13, wherein the command recorded as an "http://" request in the application content corresponding to the second reliable context is determined as the reliable request, and the command recorded as an "httpu://" request in the application content corresponding to the second reliable context is determined as the unreliable request.

15-48. (CANCELLED)

49. (CURRENTLY AMENDED) The method of claim 3, wherein the application content is a Java-program written in the Java programming language, a script program, or a markup document.

50. (CURRENTLY AMENDED) The method of claim 12, wherein the application content is a Java-program written in the Java programming language, a script program, or a markup document.